SECURE PROCESSING UNIT SYSTEMS AND METHODS

ABSTRACT OF THE DISCLOSURE

A hardware Secure Processing Unit (SPU) is described that can perform both security functions and other information appliance functions using the same set of hardware resources. Because the additional hardware required to support security functions is a relatively small fraction of the overall device hardware, this type of SPU can be competitive with ordinary non-secure CPUs or microcontrollers that perform the same functions. A set of minimal initialization and management hardware and software is added to, e.g., a standard CPU/microcontroller. The additional hardware and/or software creates an SPU environment and performs the functions needed to virtualize the SPU's hardware resources so that they can be shared between security functions and other functions performed by the same CPU.